UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEIZURE OF ALL USDT TOKENS HELD IN TWO CRYPTOCURRENCY WALLET ADDRESSES IDENTIFIED BY: **0x966913c26ab93a856f4b2372ecf6ba46a76e2b57** **TPT4pz7g697maRahjUBvZHeSz2xvBaFCe6**	**1:25-sw-12**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

I, Michael Imbler, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for the equivalent value of USDT (the "**Subject Funds**") stored in the following cryptocurrency wallet addresses (the "**Subject Addresses"**):

   a. All Tether ("USDT") held in a wallet address identified by 0x966913c26ab93a856f4b2372ecf6ba46a76e2b57 ("**SUBJECT ADDRESS 1**")

   b. All Tether ("USDT") held in a wallet address identified by TPT4pz7g697maRahjUBvZHeSz2xvBaFCe6 ("**SUBJECT ADDRESS 2**")

The particular items to be seized are described in the following paragraphs and in Attachment A.

2. I have been employed as a Special Agent of the FBI since August 2007 and am currently assigned to the Washington Field Office, Northern Virginia Resident Agency, Asset Forfeiture Squad. Since joining the FBI, I have investigated violations of federal law involving

matters of national security and espionage. At the start of my employment, I received training on how to conduct criminal investigations at the FBI Academy in Quantico, Virginia. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants, seizures, and the identification and collection of evidence. From my training and experience, I have also become familiar with the techniques and methods utilized by criminal enterprises to evade law enforcement while conducting criminal activity, to include many ways to launder proceeds from illicit activity or forms of communication utilized to avoid law enforcement detection.

3. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. As further described below, this affidavit is made in support of an application for a seizure warrant for funds traceable to, and involved in, a fraud scheme that deceived multiple victims into sending cryptocurrency payments to fraudulent platforms, for which payments were subsequently laundered into the **SUBJECT ADDRESSES**. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that unknown subjects have violated 18 U.S.C. §§ 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and laundered the proceeds of that activity in violation of 18 U.S.C. § 1956(a)(1)(B)(i), 18 U.S.C. § 1957, and 18 U.S.C. § 1956(h) (money laundering,

violation of the spending statute, and conspiracy to commit money laundering). There is also probable cause to believe that the **SUBJECT ADDRESSES** received the proceeds of the wire fraud scheme described below and that the **SUBJECT FUNDS** are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). Moreover, there is probable cause to believe that the **SUBJECT FUNDS** are subject to forfeiture as property involved in money laundering offenses, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

APPLICABLE LAW

A. Substantive Criminal Offenses

5. Wire fraud: 18 U.S.C. § 1343 makes it a crime for anyone, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

6. Title 18 U.S.C. § 1349 punishes any attempt or conspiracy to violate, *inter alia*, 18 U.S.C. § 1343.

7. Concealment money laundering: 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

8. The Spending Statute: 18 U.S.C. § 1957 provides in relevant part that "[w]hoever . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity" shall be guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, § 1957 is sometimes referred to as the Spending Statute. Violations of § 1957 are considered money laundering offenses.

9. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate 18 U.S.C. § 1956 or 18 U.S.C. § 1957.

B. Asset Forfeiture Statutes

10. The proceeds of wire fraud are subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity ("SUA"), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA is subject to civil forfeiture. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343. In addition, 28 U.S.C. § 2461(c) provides that, "[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized," then the government can obtain forfeiture of property "as part of the sentence in the criminal case." Thus, pursuant to 28 U.S.C. § 2461(c) and 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to wire fraud is subject to criminal forfeiture.

11. Property involved in a money laundering offense is subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 or 1957, or any property traceable to such property, is subject to civil forfeiture. In addition, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in a violation of 18 U.S.C. §§ 1956 or 1957, or any property traceable to such property, is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. Forfeitures encompass all property "involved in" the crime, which can include untainted funds that are comingled with tainted funds derived from illicit sources. See United States v. Casey, 444 F.3d 1071, 1073 (9th Cir. 2006) ("It is . . . clear that Congress intended criminal forfeiture provisions to eliminate profit from certain criminal activities, including money laundering . . . ."); United States v. Kivanc, 714 F.3d 782, 794-95 (4th Cir. 2013) ("Consequently, when legitimate funds are commingled with property involved in money laundering or purchased with criminally derived proceeds, the entire property, including the legitimate funds, is subject to forfeiture."); United States v. Guerrero, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) ("[C]ommingling 'clean' money with crime proceeds can 'make[ ] money laundering less difficult and may even be necessary to the successful completion of the offense.' . . . As a result, courts have found that untainted funds are 'involved for purposes of the forfeiture statute.'" (internal citations omitted)); United States v. Lazarenko, 564 F.3d 1026, 1035 (9th Cir. 2009) ("[I]n a money laundering charge, the commingling of tainted money with clean money taints the entire account. The money transferred from a commingled account does not need to be traceable to fraud, theft, or any wrongdoing at all. It is enough that the money, even if innocently obtained, was commingled in an account with money that was obtained

illegally.") (internal citations omitted). Moreover, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of those same two offenses is subject to forfeiture pursuant to 18 U.S.C. § 982(a)(1), 18 U.S.C. § 981(a)(1)(A), and 28 U.S.C. § 2461(c).

12. This application seeks a seizure warrant under both civil and criminal authority, because the property to be seized could easily be placed beyond process if not seized by warrant, as cryptocurrency is fungible and easily dissipated.

13. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(l) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. Title 21 U.S.C. § 853(f) permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture. The seizure warrant issues if the Court determines that there is probable cause to believe that the property seized would, in the event of conviction, be subject to forfeiture and that a restraining order may not be sufficient to assure the availability of such property for forfeiture.

BACKGROUND

Definitions

14. **Virtual Currency:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of

traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

15. **Virtual Currency Address:** A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

16. **Virtual Currency Wallet:** A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

17. **Virtual Currency Exchange:** A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of

stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

18. **Blockchain:** Many virtual currencies publicly record their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

19. **Blockchain Analysis:** Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

20. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

21. **Tether (USDT):** Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

22. **Ether:** Ether ("ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

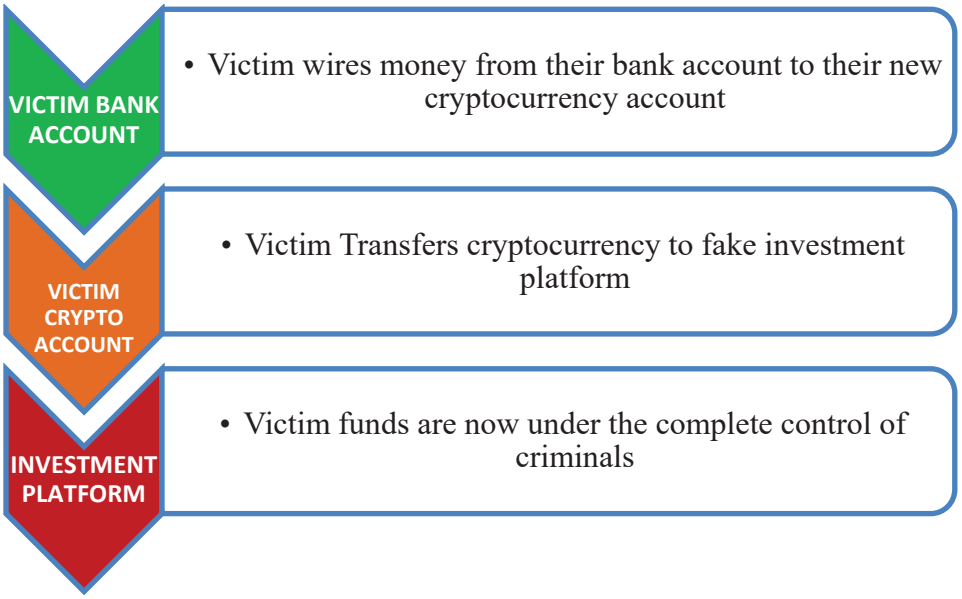
23. **Tron:** Tron ("TRX") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving TRX are publicly recorded on the Tron blockchain, which allows anyone to track the movement of TRX.

24. **Bitcoin:** Bitcoin (or "BTC") is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

25. **Cryptocurrency Investment Schemes ("Pig Butchering"):** The FBI is investigating an investment fraud scheme, referred to as "pig butchering," a term derived from the foreign-language word used to describe this scheme. Based on data submitted to the FBI's Internet Crime Complaint Center (located at https://www.ic3.gov/) in 2022 alone, pig butchering schemes targeted tens of thousands of victims in the United States and resulted in over two billion dollars in private assets being siphoned overseas. Pig butchering schemes begin by criminals contacting potential victims through seemingly misdirected text messages, dating applications, or professional meetup groups. Next, using various means of manipulation, the

criminal gains the victim's affection and trust. Criminals refer to victims as "pigs" at this stage because they concoct elaborate stories to "fatten up" their victims.

26. Once that trust is established, the criminal recommends cryptocurrency investment by touting their own, or an associate's, success in the field. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake investment platform hosted on a website. These websites, and the investment platforms hosted there, are created by criminals to mimic legitimate platforms. The subject assists the victim with opening a cryptocurrency account, often on a U.S.-based exchange such as Coinbase, Crypto.com or Kraken, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform. On its surface, the platform shows lucrative returns, encouraging further investment; underneath, all deposited funds are routed to a cryptocurrency wallet address controlled completely by the criminals – the "butchering" phase of the scheme.



27. Pig butchering perpetrators frequently allow victims to withdraw some of their "profits" early in the scheme to engender trust and help convince victims of the legitimacy of the

platform. As the scheme continues, victims are unable to withdraw their funds and are provided various excuses as to why. For example, the criminals will often levy a fake "tax" requirement, stating taxes must be paid on the proceeds generated from the platform. This is just an eleventh-hour effort by the criminals to elicit more money from victims. Ultimately, victims are locked out of their accounts and lose all their funds.

28. The cryptocurrency ecosystem is used by criminals not only to receive victim money, but to launder it quickly, anonymously, and at scale. Like traditional money laundering, laundering money through cryptocurrency shares the same three stages of placement, layering, and integration, with different techniques applied within each:

- **Placement –** Criminals use non-custodial, or "private" wallets to initially receive victim funds. This is because such wallets are unattributable to law enforcement by blockchain analysis alone, are simple to create, and can accept large transaction amounts without additional scrutiny.
- **Layering –** Next, criminals will have victim funds transverse numerous private wallets, consolidate with other illegitimate and sometimes legitimate funds, and be subjected to other more cryptocurrency-specific processes to obfuscate both the origin of, and the ultimate destination for, the victim funds.
- **Integration –** Finally, by using a diffuse network of "brokers," who agree to exchange cryptocurrency for fiat using various means, criminals render their proceeds liquid and fully integrated with the legitimate financial system.

PROBABLE CAUSE

29. On or about November 27, 2024, VICTIM 1, a resident of the Eastern District of Virginia, reported a pig butchering investment scam to the FBI. Starting in or around early

October of 2024, VICTIM 1 saw an advertisement on Instagram for an investment club. VICTIM 1 clicked on the ad, which routed VICTIM 1 to a WhatsApp group named "The MOND Club". Within this group, VICTIM 1 met an individual claiming to be named 'Elisa Jones', who sent VICTIM 1 a link and referral code for an investment app created by MOND Technology Co., Ltd. (MOND).

30. VICTIM 1 provided a screenshot of the WhatsApp profile for 'Elsa Jones', which included an image of a woman and a phone number.

31. A reverse image search of the profile picture reveals that the origin of this picture is not, in fact, of an individual named 'Elsa Jones', but a Turkish media personality and presenter. The image can be seen on the Turkish media personality and presenter's Instagram page.

32. Furthermore, this same image, and general facts of this scam, can be seen in a recent Youtube video posted by the channel Christope[1], in which journalist Christophe Haubursin investigates cryptocurrency scams and pig butchering. Within their investigation, they encounter a scam with similar methodologies, in which the assistant that they speak to is named 'Daisy Carey', and uses the same WhatsApp profile picture, stolen from a Turkish media personality and presenter, as 'Elisa Jones'.

33. Through MOND, VICTIM 1 began purchasing a small amount of cryptocurrency, in the form of Tether (USDT) through their personal Cryptocurrency exchange account at Coinbase, in order to invest the USDT with MOND. MOND claimed to have various ways of investing USDT pegged to other tokens and coins, all of which were determined by an individual

[1] The channel can be viewed at https://www.youtube.com/@christophe, while the specific video referenced is located at https://www.youtube.com/watch?v=1QhMqoTNSl8

associated with MOND, generally referred to as 'The Professor'. MOND's website identifies 'The Professor' as an individual named 'Mason Kenny'. 'The Professor' would determine what coins/tokens constituted good investments, which would be relayed to 'Elisa Jones', who in turn would inform VICTIM 1 of these supposed investment opportunities.

34. MOND Technology Co., Ltd is a business that is a registered business in Colorado. It was registered on or about July 26, 2022, with a physical street address located on Yosemite St, Suite 120, in Denver, Colorado. The registered agent listed is Shuaijian Zhang, whose listed mailing address is the same as the physical address as MOND Technology.

35. On or about August 1, 2022, approximately 4 days after registering as a business in Colorado, MOND Technology registered with FinCEN as a Money Service Business (MSB).

36. A google search of the Yosemite St. address revealed that the address is a business park owned by a real estate investment firm located in Miami, FL, whose website identifies this as 'Yosemite Office Plaza". Further google searches reveal that suite 120 within the office park, the purported location of MOND Technology, is in fact an office location for a company which specializes in property management within the state of Colorado.

37. Both the owner of the property located on Yosemite St. and the company currently located in Suite 120 were contacted, and both confirmed that MOND is not currently and has never been—since August 2022—a tenant of Suite 120.

38. Based on my training and experience, I know that it is common for many similar fake investment platforms to register fake businesses within the United States to dupe those who they wish to victimize. In all likelihood, MOND simply used this address to register the business and apply for a FinCEN MSB registration to appear legitimate in the eyes of prospective victims of their scam.

39. Between on or about October 8, 2024, through on or about November 4, 2024, VICTIM 1 conducted approximately 12 transactions investing approximately 41,678.50612 USDT, valued at about $41,678.50.

40. On or about November 4, 2024, VICTIM 1 attempted to withdraw some of their investments for the first time. Upon this attempt, VICTIM 1 was told by MOND Customer Support that they were unable to withdraw any of their funds, and that in order to submit a withdrawal request, VICTIM 1 must first pay a 20% fee. VICTIM 1 eventually paid this fee and was then told they must wait in a queue to withdraw their funds, and that their current position in the queue was 18868. VICTIM 1 was told that they could pay a "fast track fee" in order to get a higher spot in that queue. VICTIM 1 paid this fee as well. However, at no point did VICTIM 1 receive any amount of the funds they had invested. VICTIM 1 was instead repeatedly told they remained in the queue, and asked to pay more "fast track fees" or "commissions" to receive their funds.

41. Between on or about November 4, 2024, through on or about December 1, 2024, VICTIM 1 paid a total of approximately 6 fees, worth approximately 53,244.69 USDT, valued at about $53,244.69.

42. Based on my training and experience, the overall structure of these investments and fee requirements is consistent with the same or similar frequently used tactics by Pig Butchering scams. The intent is to create a sense of panic and desperation in the victims so that they continue to invest and pay fees. Victims often feel that they have already invested so much that they need to continue until they realize some sort of profit, otherwise, it would have all been for nothing.

43. In all, VICTIM 1 invested and/or paid fees totaling approximately 94,923.20 USDT, valued at about $94,923.20. At no point since beginning to invest until the present time has VICTIM 1 had their investments returned to them, nor has VICTIM 1 been reimbursed for any of the fees paid.

SUMMARY OF MONEY LAUNDERING ACTIVITY

44. Investigators used blockchain analysis to trace VICTIM 1's payments on the blockchain and identified a network of cryptocurrency addresses used to receive and launder VICTIM 1's payments, as well as receive and launder the funds of victims of the same or similar pig butchering scams. The investigation revealed that this network of scammers received victim funds primarily in the form of USDT on the Ethereum blockchain. The funds were then sent through various addresses in a manner designed to obfuscate the flow of funds before they were ultimately deposited into the **SUBJECT ADDRESSES.**

Victim Payments in USDT Are Sent to Consolidation Addresses

45. Based on my training and experience, I know that pig butchering scammers/money launderers typically set up individual cryptocurrency addresses for each, or a small group, of victim(s), to use to send funds to the fraudulent investment platform. After a victim sends funds to a unique cryptocurrency address provided by the scammers, the scammers usually move the funds to another address within minutes or hours of the victim's deposit. Frequently, the funds are then quickly moved into "consolidation addresses," which consolidate the funds sent by various victims. In this situation, VICTIM 1 was provided multiple deposit addresses, each being used almost exclusively by VICTIM 1.

46. Between on or about October 8, 2024, through on or about December 1, 2024, VICTIM 1 used an account at the cryptocurrency exchange Coinbase to send 18 transactions

totaling 94,923.2004 USDT. These 18 transactions were sent to four different addresses provided to VICTIM 1, which VICTIM 1 believed to be their deposit addresses for MOND. However, in reality, the addresses were not connected to any investment platform, and were instead controlled exclusively by the individual(s) perpetrating the scam. Therefore, these addresses are herein referenced as "Deposit Addresses" (DA).

47. Of the 18 transactions, 13 transactions, totaling approximately 62,573.99867 USDT, were sent to DA 0x4f6cf39881ec1168a1694093a6025415934285e4 (DA 1); 1 transaction, totaling approximately 6,204.436172 USDT, was sent to DA 0x65f74839a203df22ef2105f37d677ca09c5f3d72 (DA 2); 1 transaction, totaling approximately 6,000.630066 USDT, was sent to FDA 0x6e7d7df997c0df60e2e73006225f73ac6b0190f5 (DA 3); and 3 transactions, totaling approximately 20,144.13549 USDT were sent to DA 0xa128e848492bdeef1731781a94e7c660a6746ac4 (DA 4). A table of these transactions can be seen below:

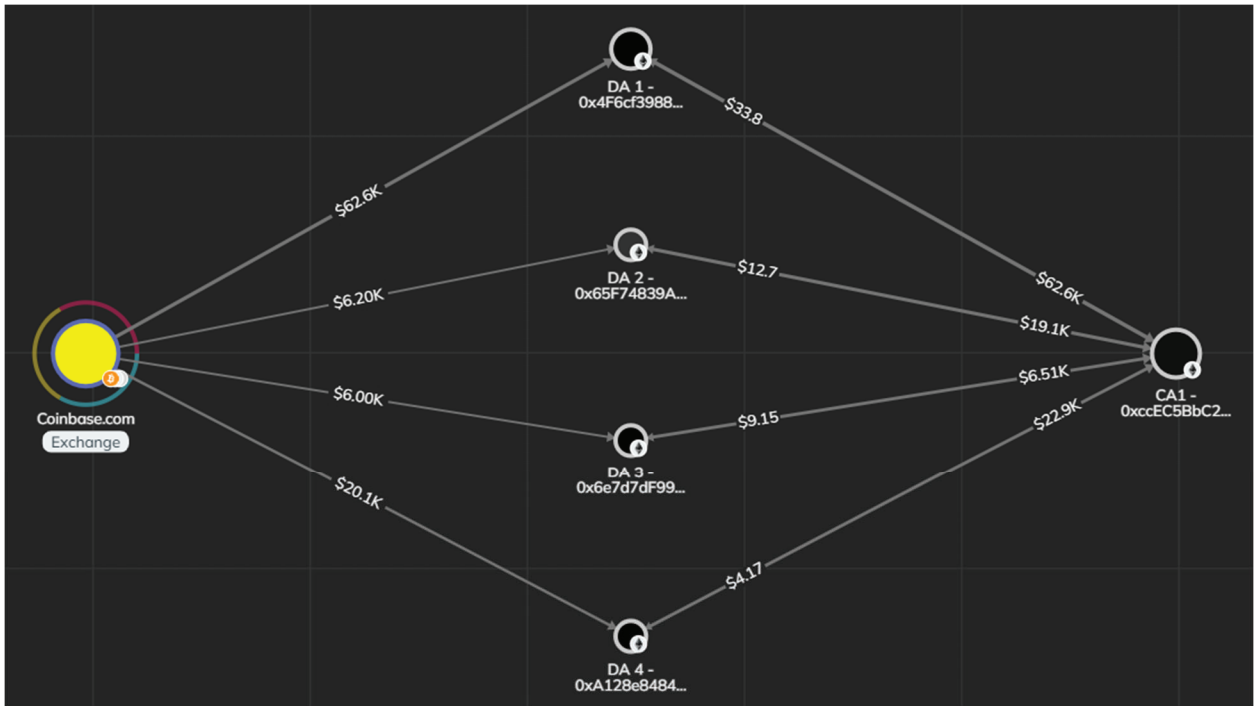
Date	Amount	Hash	Sent To
10/8/2024 0:42	100.028508	0xc96b525cb5a6af4682bdd6ddaf54d44e57a7d2941cfa0ce59c755eb374a9b18c	DA 1
10/8/2024 21:38	60.045334	0xe08050a63702bc50bb6eed8c02d0794c89d945af4bca82e098408bf14231dc1e	DA 1
10/8/2024 22:13	300.217658	0x2f2a81955ef972afd21110b9864c81543ac70a1e4a03b04839811615b312ee8b	DA 1
10/11/2024 19:44	600.18906	0xe1275c2f0ef7db5dc28a96ceac7b52a6e6481dc4cfd6bd302888329c68022096	DA 1
10/13/2024 12:09	1,908.04	0xc2c3f4836f2ad71a26ca36ad39a37f9f5d7288f0d9c4b6e6cdc6133be426b29a	DA 1
10/14/2024 22:09	2,500.39	0xa6930904212c1bd5208237b034957828ee360ca145f5a5f53a642f424d5d09a2	DA 1
10/17/2024 0:26	2,488.75	0x9bf01f669c365e77f06c1247b05bf43377c9c07968f2266ef126012fc6ee6e27	DA 1
10/17/2024 2:39	1,500.50	0xd7d7926209ba096420683c41edd5c013e4986a51d7319738b298adb498d080f4	DA 1
10/22/2024 2:31	10,006.05	0xdd7993cdd462b87290ff01f838eae7f6074eac85bacc850fcb4d1d50b62b7da8	DA 1
10/29/2024 1:42	5,184.72	0x87578ae329704c973d7dfd386d2797798698819dd98a59ff6c1695ae1dcabf2e	DA 1
10/29/2024 19:56	9,982.50	0x443d8c5600cfaf58bf2d5c50187da6b64af6d963c52025dbf9457dc719bd4d67	DA 1
10/30/2024 8:03	7,047.06	0x20e2a841e386a23e12de1c98876e1fd47125cd95bfb0e12f172e64499a9e2f2e	DA 1
11/4/2024 21:59	6,204.44	0x822e41e0976e38198b90d497c77455c1fb88a53b70e09cb9275226f970179b57	DA 2
11/14/2024 21:22	6,000.63	0xa2f9ba278bb393e1de093fadca9ee67e8c637a5d1d861351f05bdbaec5c6eb75	DA 3
11/15/2024 22:16	9,996.05	0x95e104d7452ebd6a66cb832375b104fe545e7b5a91a5d176a091464a0e9270cd	DA 4
11/15/2024 22:17	10.00	0x2f914f394bdc8ba92983e9c24524b57d730a3b201a02f5b337b07bd4b5f2462c	DA 4
11/25/2024 20:44	10,138.09	0x9725feffeec9afddea90896ee014fd53cc4823080905c22290cfef941ee48afd	DA 4

11/30/2024 20:05	20,895.49	0xe266aa7fa3b1c8b415a7673b1a49ac28193809661933f813865bacc52886a620	DA 1

48. After receiving VICTIM 1's payments, each of the above DA's conducted almost immediate corresponding payments to a consolidation address (CA) 0xccEC5BbC20bF95f992620014C6Cc2E361FA1a8E3 (CA 1). Between on or about October 8, 2024, through on or about December 1, 2024, DA 1, DA 2, DA 3, and DA 4 each sent the totality of VICTIM 1's deposits to CA 1, which in turn received 100% of VICTIM 1's deposits. A table of these transactions is included below:

Date	Amount	Hash	From	To
10/8/2024 1:43	100.028508	0x5ed0a8a70535a0e95c89c318a43fa2f62786c8fb40d1f4f6b2087e600343b497	DA 1	CA 1
10/12/2024 22:36	960.452052	0xba9e969b9d459dbae1985d3e3e8e14ddf51e797af67442c09e7e790bba61605a	DA 1	CA 1
10/14/2024 15:56	1,908.04	0x319d99b8df7864e4ca3b633727e4cc750b3eb216920bbeb1bcfc6a836d57ce1a	DA 1	CA 1
10/15/2024 18:06	2,500.39	0xfc490d3804b911cd57b2c3e69503a86166e882169268b5840bfa1d2ec86c9a78	DA 1	CA 1
10/17/2024 15:22	3,989.25	0x4bd92bbebb5d477de1be01e9b987db01e2d75793de53061fabd95c368ab03dd6	DA 1	CA 1
10/23/2024 1:02	10,006.05	0x8845d151a15123f337da092c2fa7d19f504257fea9dd4f36afd9e2887e9e18e4	DA 1	CA 1
10/29/2024 20:04	15,167.23	0x7688b8ef4bc1c9a46b6db972e30d1e932d0a478bc294868005873c3e87ee97e5	DA 1	CA 1
11/10/2024 19:52	7,047.06	0xb4675645b0332b6358c9aac4e97f3e8fe79300d69c025419639f4ab33e483a23	DA 1	CA 1
11/10/2024 19:52	6,204.44	0x57d800b1f0902a56864453361af8da480f393be35f1470d77613f321474bd63e	DA 2	CA 1
11/15/2024 16:28	6,000.63	0x4dc80a6b56a07675947efa858d46750b99f4669522d93908825b6f8695705932	DA 3	CA 1
11/25/2024 20:58	22,197.14	0x0dd4aa85a57aae0b9e6c10d386551d49e517bece2f6d26a026444f0a3f7c13fe	DA 4	CA 1
12/1/2024 19:04	20,895.49	0x8f7a4ae6aef4df68f0bfed3c6a197b722b2adb6e9ee63a56f05b72f3bfe23cc9	DA 1	CA 1

49. A visual depiction of the totality of the above transfers represented in the tables in paragraphs 47 and 48 can be seen below:



50. Based on my knowledge and experience, Consolidation Addresses are used frequently by Pig Butchering organizations. While the deposit addresses that are provided to the victims are typically unique to that victim, the consolidation address(es) are not. Instead, these consolidation addresses serve as repositories for many victim's funds to be held in one location and moved in larger sums. Consolidation Addresses make the movement and laundering of the victim funds faster and easier while also reducing the number of transactions required to move all of the funds, and therefore reducing the associated fees required for each transaction.

51. Furthermore, victim payments into pig butchering networks typically share a similar profile – victims make payments directly from a centralized exchange into an address that is controlled by scammers. The scammers then almost immediately sweep the victim payments into a consolidation address, which will receive victim payments from dozens of victims. In the current network, the vast majority cryptocurrency addresses that sent funds to CA 1 shared this

profile – each address received transactions directly from likely individual victim wallets, funded by payments from cryptocurrency exchanges. These wallets also passed the entirety of the funds deposited into the victim addresses to CA 1.

52. In this case, CA 1 has operated between approximately July 30, 2024 and the present day. From on or about July 30, 2024 and the final deposit of VICTIM 1, to on or about December 1, 2024, CA 1 received a total of about 194,819.1233 USDT, valued at about $194,819.12. These funds were received from approximately 40 unique addresses, which includes DA 1-4. VICTIM 1's funds represent almost half (about 48%) of the total funds received by CA 1 during this period of time. If adjusted for the period of time that VICTIM 1 was actively being scammed, CA 1 received a total of approximately 162,100.4185 USDT, of which VICTIM 1's funds represent about 58.5%.

53. Based on my knowledge and experience, Pig Butchering networks often utilize multiple consolidation addresses as part of the layering stage of the money laundering. While the entirety of the fraudulently obtained funds may not be sent to consolidation addresses, the majority of them will be.

54. Of the about 162,100.4185 USDT CA 1 receives between on or about October 8, 2024, and on or about December 1, 2024, approximately 126,000 USDT is sent to 0x966913c26ab93a856f4b2372ecf6ba46a76e2b57 (SUBJECT ADDRESS 1). Specifically, the transactions sent from CA to SUBJECT ADDRESS 1 that include victim funds are:

Date	Amount	Hash	From	To
10/8/2024 1:57	10,000	0x4ee50d29ccfabdaa7e1097710da064ac0f6ab43f0cb00529634410b913a5d167	CA 1	SA 1
10/17/2024 15:29	3,000	0xb166827ab82f642c920005b0a96dc0e04f2a2bf44a199fafc86eec2f54240b5d	CA 1	SA 1
10/22/2024 15:05	11,000	0x03ac7588b46164535e1251b5e4948af3f34a10174a4dc86b3d55c8aa7166e95f	CA 1	SA 1
10/26/2024 1:46	10,000	0x9f433adf853d1e074a5b68eb536dca09e386cdc363bd1fecedcf3a9b45799c48	CA 1	SA 1
11/2/2024 16:22	20,000	0xda47d62606ee94488bf443c03b8c3b8691349413ddf0724ee0b76b40d2268957	CA 1	SA 1
11/10/2024 19:59	12,000	0x9849004ac2b7a1b431fcbd5e8c5ee07aead3effe31a278c7f161c54445d47bff	CA 1	SA 1

11/10/2024 23:26	10,000	0x9d8e0453913302dc46c5c9065a5b99f5b7d4701ed43ce77b645beeb3c470e50b	SA 1	CA 1
11/26/2024 16:23	34,000	0xa8d759f577768b720bda7359d6cf6e2c431e60fc6a70a98e9d2363ca73c1724e	CA 1	SA 1
12/1/2024 19:09	26,000	0xe0dab2c493c49acc974dd7c1cc4bb9b339a93f654d5006160a408f55e0369369	CA 1	SA 1

55. It should be noted that of the approximately 12,000 USDT that is sent from CA 1 to SA 1 on or about November 10, 2024, approximately 10,000 USDT is returned from SA 1 to CA 1 within hours of the transfer. No additional transfers to or from SA 1 occurred between those transfers.

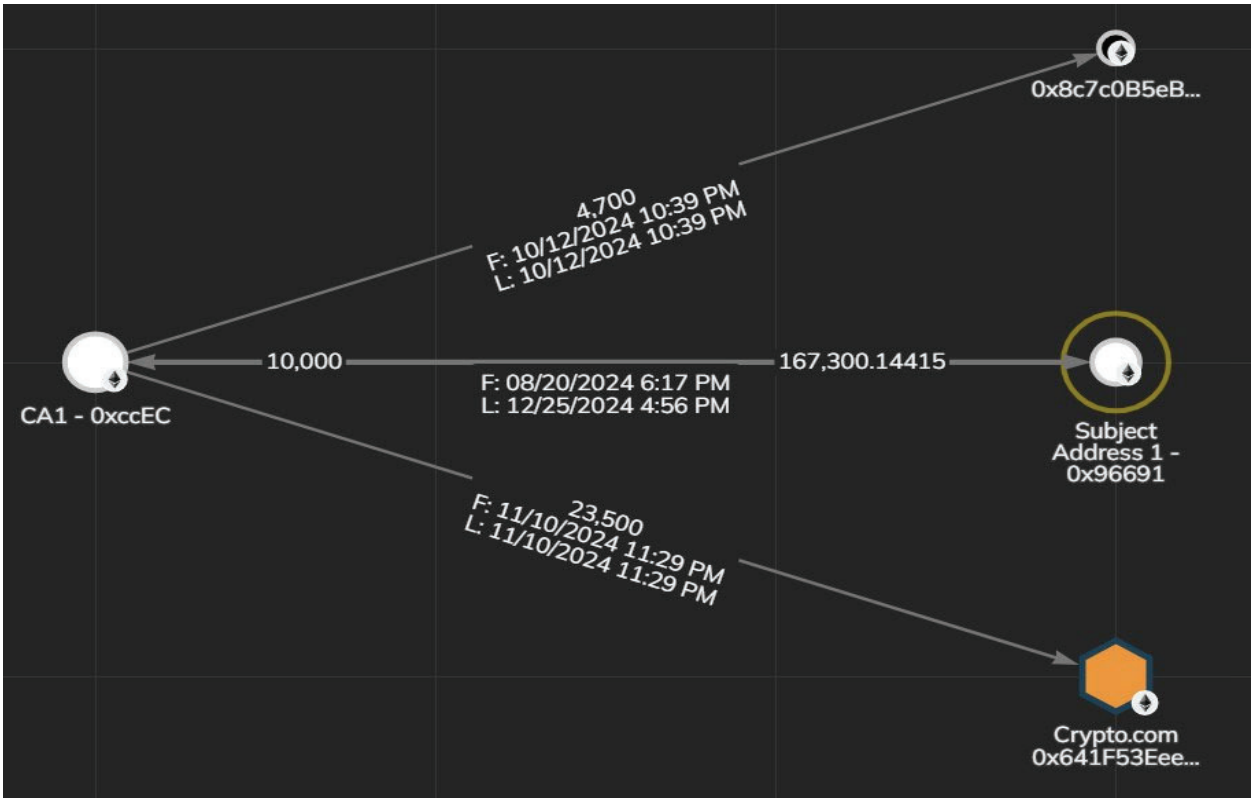
56. The government has employed the lowest intermediate balance rule ("LIBR") in analyzing the **SUBJECT ASSETS**, which is a method of tracing criminal proceeds. Under the LIBR, when criminal proceeds are commingled with other funds in an account, there is a presumption that other funds are withdrawn first, leaving the criminal proceeds in the account. Under the presumption, criminal proceeds remain in the account as long as the account balance is equal to or greater than the amount of criminal proceeds deposited. See Sony Corporation of America v. Bank One, West Virginia, Huntington, NA, 85 F. 3d 131 (4th Cir. 1996). However, that does not mean that the LIBR requires that the proceeds are always spent last. See United States v. Miller, 911 F.3d 229, 234 (4th Cir. 2018). "In other words, the LIBR circumscribes what can be traced into an account, rather than out of it." Id. at 235. The Fourth Circuit described the LIBR in Miller as follows:

> The LIBR provides that where the balance of an account into which tainted proceeds are deposited subsequently dips below the amount of those tainted proceeds, the only tainted funds thereafter traceable to the account are funds equal to that lowest account balance. This is true even if the account balance later grows through the deposit of legitimate funds. Assume, for example, that a money launderer deposits $50,000 of laundered proceeds into an account with a balance of $100,000, yielding a new balance of $150,000. The launderer then spends $120,000 and buys, inter alia, a $20,000 car, leaving the account with only a $30,000 balance. The LIBR precludes ascribing more than $30,000 in laundered

> proceeds to that bank account thereafter, even if the balance of the account subsequently rises above $50,000 through the deposit of legitimate proceeds. However, it permits tracing $20,000 to the car that the money launderer purchased with tainted funds.

Id. at 234 (4th Cir. 2018).

57. Using the Lowest Intermediate Balance Rule (LIBR), the transfers from CA 1 to **SUBJECT ADDRESS 1** contain approximately 83,850.15763USDT worth of VICTIM 1's funds. CA 1 additionally sends one transfer of approximately 4,700 USDT (containing about 921.95706USDT of VICTIM 1's funds) to 0x8c7c0b5eba6731fbd29fd152b1d57610957f44ed and sends one transfer of approximately 23,500 USDT (containing about 11,251.49974 USDT of VICTIM 1's funds) to 0x641f53eeef098a5e769ec548b1de9b0854765edc, an address associated with the exchange Crypto.com. This is depicted in the below image:



58. **SUBJECT ADDRESS 1** was active between on or about August 20, 2024, through on or about December 8, 2024. During this period of time, **SUBJECT ADDRESS 1**

received USDT deposits from three individual addresses, totaling approximately 156,669.14415 USDT. Of that, approximately 152,300.14415 USDT came from CA 1. The remaining 4,369 USDT came from two addresses with activity that is consistent with other consolidation addresses.

59. **SUBJECT ADDRESS 1** transferred funds to only three addresses, CA 1, 0xE9422791603CB6375f0aC21FDD16dD2663793649, an address associated with the Exchange OKX and 0x1f78a99371014270F32Fb9d9c4Ca0e74CB0E57ee, an address associated with the exchange Binance.

60. On or about October 18, 2024, **SUBJECT ADDRESS 1** transferred approximately 31,000 USDT to 0xE9422791603CB6375f0aC21FDD16dD2663793649. Using the LIBR rule, at the time of the transfer, this transfer contained approximately 925.2746 USDT of VICTIM 1's funds. The remaining funds in this transfer came from funds held in CA 1 that were obtained prior to VICTIM 1's involvement with the scam.

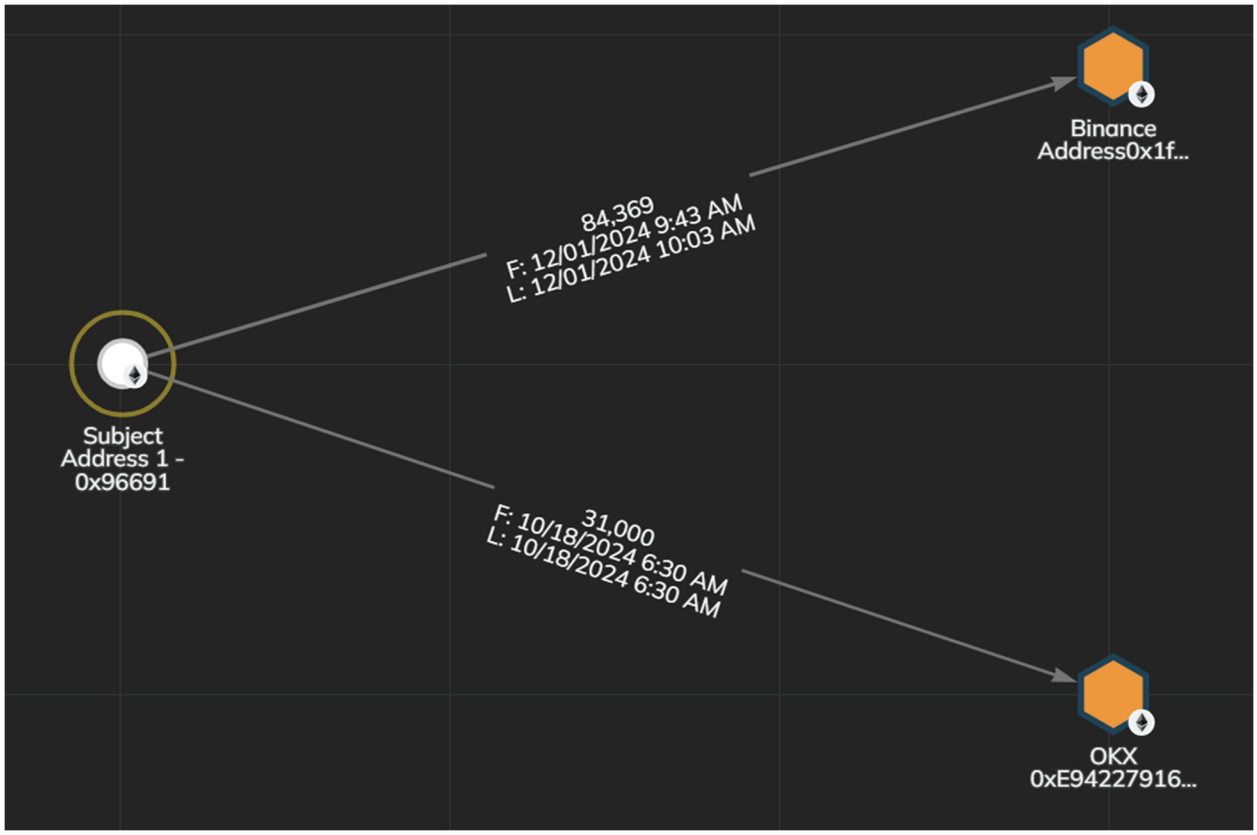
61. On or about November 10, 2024, **SUBJECT ADDRESS 1** transferred approximately 10,000 USDT to CA 1. At the time of this transfer, **SUBJECT ADDRESS 1** held a balance of approximately 53,000 USDT, all of which came directly from CA 1. The transfer of about 10,000 USDT from **SUBJECT ADDRESS 1** was, therefore, simply the return of about 10,000 USDT to CA 1. The approximately 10,000 USDT was subsequently included in the transfer of 23,500 USDT from CA 1 to 0x641f53eeef098a5e769ec548b1de9b0854765edc, the address associated with Crypto.com, which was described above. Following this transaction, **SUBJECT ADDRESS 1** held a balance of approximately 43,000 USDT.

62. Following the transactions described in paragraphs 60 and 61, four additional transactions are sent to **SUBJECT ADDRESS 1**, including the aforementioned about 4,369

USDT from the other two addresses **SUBJECT ADDRESS 1** interacts with, and approximately 34,000 USDT from CA 1, which includes victim funds. Following these transactions, the **SUBJECT ADDRESS 1** held a balance of approximately 84,369 USDT.

63. On or about December 1, 2024, **SUBJECT ADDRESS 1** conducted two transactions, both sent to address 0x1f78a99371014270f32fb9d9c4ca0e74cb0e57ee, an address associated with the Binance.com exchange, herein referred to as Binance Address 1 (BA 1). At the time, these transactions depleted all funds held within **SUBJECT ADDRESS 1**.

Date	Amount	Hash	From	To
12/1/2024 9:43	14,369	0x92b10bf69e4de79f3892aad0ff6c16da311c7d7a3395971d2c6357186a01f2eb	SA 1	BA 1
12/1/2024 10:03	70,000	0xb5822262a8e18624dab0e65acc00907f63419ae5dc9574729b4514845c555442	SA 1	BA 1



64. Based on my training and experience, individuals associated with pig butchering scams will accept various types of cryptocurrency from victims before ultimately swapping into

whatever format is preferred before laundering and cashing out. Furthermore, not only will individuals associated with pig butchering scams swap cryptocurrency types, but they will also attempt to move the cryptocurrency from one blockchain to a different one, an action known as "blockchain hopping" or "bridging".

65. In order to move from one blockchain to another, individuals must utilize a service, be that a bridging service or an exchange. Typically, in pig butchering investigations, individuals will bridge cryptocurrency using an exchange. Swapping cryptocurrency and engaging in blockchain hopping or bridging further obfuscates the origin of the cryptocurrency and causes the tracing of the cryptocurrency to become more complex. Based on my training and experience, I know that quick swaps from one type of cryptocurrency to another and bridging is a strong indication that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

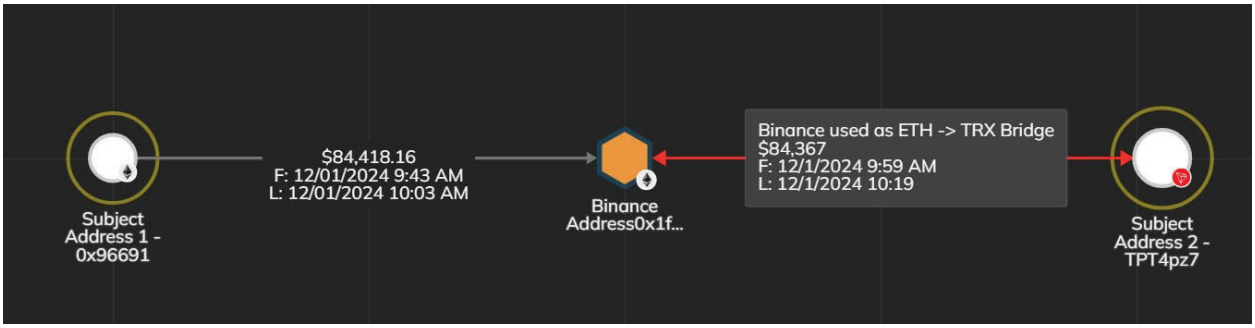
66. Law Enforcement obtained records related to BA 1 and reviewed the contents. BA 1 is associated with a Binance Account held by R.C., a Cambodian national. A Cambodian ID card was provided to Binance as proof of identity. Access logs for this Binance account show that every single time this account was accessed, it was done so using IP addresses that resolve to Cambodia, specifically, P.P. Based on my training and experience, Cambodia, among other countries in and around the South East Asia and China region, are countries and regions in which pig butchering originated and are areas that have heavy traffic related to pig butchering scams.

67. A review of the transaction history of BA 1 shows that, at the time the funds sent from **SUBJECT ADDRESS 1** were deposited, BA 1 held a balance of approximately 0 USDT. Within minutes of each deposit from **SUBECT ADDRESS 1** to BA 1, the USDT was bridged

from the Ethereum blockchain to the Tron blockchain and withdrawn to address TPT4pz7g697maRahjUBvZHeSz2xvBaFCe6 (**SUBJECT ADDRESS 2**).

Date	Amount	Hash	From	To
12/1/2024 9:43	14,369	0x92b10bf69e4de79f3892aad0ff6c16da311c7d7a3395971d2c6357186a01f2eb	SA 1	BA 1
12/1/2024 9:59	14,368	72ee9362d5af06811df990f14d1ee6ead061f8cc39658c06ad08697ca32896b5	BA 1	SA 2

Date	Amount	Hash	From	To
12/1/2024 10:03	70,000	0xb5822262a8e18624dab0e65acc00907f63419ae5dc9574729b4514845c555442	SA 1	BA 1
12/1/2024 10:19	69,999	3a21b28db498df1f35f8d5866e1720c53e2a52403d553f75646080f3cabb1b0e	BA 1	SA 2



68. **SUBJECT ADDRESS 2** has conducted transactions starting in or around May 3, 2024, to in or around December 4, 2024. Over the course of **SUBJECT ADDRESS 2's** lifespan, it has received approximately 2,622,126.149358 USDT from about 570 deposits and sent approximately 2,293,436.906626 USDT over about 441 withdrawals. Prior to the deposit of these funds, **SUBJECT ADDRESS 2** held a balance of approximately 253,014.24 USDT. Due to the activity of **SUBJECT ADDRESS 2**, it is likely that these funds are derived from other scams or scam related activity, though the sheer volume of activity makes tracing the specific funds difficult. Based on my training and experience, I know that a large number of convoluted cryptocurrency transactions in a short period of time is a strong indication that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

69. Of particular note, **SUBJECT ADDRESS 2** has a significant amount of indirect receiving exposure[2] (at least approximately 702,891.2823 USDT) (i.e., has indirectly received funds from) and a significant amount of direct (at least approximately 187,516 USDT) and indirect (at least approximately 710,604.2743 USDT) sending exposure (i.e., has sent funds directly to and indirectly to) an online service named Huione Pay/Huione Guarnetee, organizations owned/controlled by their parent company, Huione Group.

a. Huione Group was originally incorporated as Huione Currency Exchange Co., Ltd. in Cambodia in August 2014.[3] According to the most recent entry for Huione Currency Exchange Co., Ltd. in the Cambodian Corporate Registry in November 2019, the company operates a variety of business interests ranging from the wholesale trade of machinery and metal products to the operation of hotels, restaurants, and the provision of freight transport, real estate, and money changing services.[4]

b. Huione Pay, a subsidiary of Huione Group, was established in Cambodia as Huione Pay, PLC in April 2018.[5] According to its website, Huione Pay aims to bring technologically enabled financial services to the world by providing a range of financial services to individuals and corporate entities including: foreign currency exchange, remittance, deposit, withholding and

[2] Direct Exposure can be described as transactions sent directly between two entities (A to B, entity B has direct receiving exposure to A). Indirect Exposure can be described as transactions indirectly sent between to entities (A to B to C, entity C has indirect receiving exposure to entity A).

[3] According to third-party research conducted by Elliptic, a blockchain analytics company.

[4] According to third-party research conducted by Sayari, a data intelligence company, and accessible via https://www.businessregistration.moc.gov.kh/.

[5] *Id.*

payment services through the Huione App, electronic bill-pay for individuals, and point-of-sale services for corporate clients.[6]

c. Huione Crypto, a division of Huione Pay, is a Cambodian based virtual currency exchange that allows users to purchase and trade various types of virtual currencies on its platform. Huione Crypto and a U.S. incorporated related company, Huione Pay, Inc., have registered as Money Service Businesses with the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). Huione Crypto and Huione Pay, Inc. stated their intention to provide foreign exchange services to all U.S. states and territories according to their FinCEN registration documents filed in April 2023 and August 2024, respectively.

d. Huione Pay International, a division of Huione Pay, facilitates international remittances, including collections and payment services according to its website.[7] Huione Guarantee, a subsidiary of Huione Group, operates Telegram-based online peer-to-peer marketplaces hosted primarily in the Mandarin language. According to Elliptic, a blockchain analytics company, Huione Guarantee was established in June 2021.

e. According to Chainalysis, a blockchain analytics company, Huione Pay's virtual currency exchange, doing business as Huione Crypto, has facilitated $49 billion in inflows to the platform using the Ethereum and TRON cryptocurrency networks. Using blockchain analytics software, the

[6] https://www.huionepay.com.kh/, (last visited October 8, 2024).
[7] *Id.*

investigative team has seen cryptocurrency wallets associated with Huione Pay send funds to a variety of suspicious counterparties, including wallets used to facilitate frauds and scams, wallets containing cryptocurrency that has been reported as stolen, wallets sending funds to U.S. sanctioned entities, and wallets engaged in the purchase or distribution of Child Sexual Abuse Material ("CSAM") among other illicit connections. Of the various segments of suspicious funds flowing into and out of Huione Pay, funds related to cryptocurrency confidence scams, often called "pig butchering" scams, account for some of the largest.

f. U.S. law enforcement frequently performs cryptocurrency tracing for U.S. based victims who fall prey to online scams which misled them into purchasing and transferring cryptocurrency to others under false pretenses. Commonly, investigators find evidence preserved on the various blockchains used by the bad actor(s) to move the funds, which indicate how the victim funds were acquired and where the funds were sent. The process of tracing and attempting to retrieving victim funds often involves following funds from their point of origin to a destination to which law enforcement can seek to secure the funds on behalf of victims. Law enforcement typically works collaboratively with these destinations, commonly virtual currency exchanges and over-the-counter cryptocurrency brokers, to try to freeze and reclaim funds on behalf of victims.

70. Given that **SUBJECT ADDRESS 2** receives a significant amount of the funds lost by VICTIM 1, the amount of exposure **SUBJECT ADDRESS 2** has to Huione, as well as

the general movement of funds, it is likely that **SUBJECT ADDRESS 2** contains mostly if not only funds related to pig butchering and/or other scams.

71. In total, BA 1 transferred a total of approximately 84,367 USDT to **SUBJECT ADDRESS 2**, of which, approximately 60,901.6696 USDT is directly traceable to VICTIM 1. Following the transfers from BA 1 to **SUBJECT ADDRESS 2** on or about December 1, 2024, **SUBJECT ADDRESS 2's** USDT balance grew from about 252,690.24 USDT to approximately 337,057.24 USDT. On or about December 1, 2024 and on or about December 2, 2024, **SUBJECT ADDRESS 2** sent approximately 20,546 USDT to other addresses and received an additional 11,070.00 USDT from other addresses, bringing its balance to approximately 327,581.242732 USDT on about December 2, 2024.

72. On December 2, 2024, the FBI requested Tether freeze the USDT remaining in **SUBJECT ADDRESS 2**. On the same date, Tether confirmed the addresses were blacklisted, the USDT was frozen, and the balance in **SUBJECT ACCOUNT 2** was 327,581.242732 USDT. Following the freeze, **SUBJECT ADDRESS 2** received one additional deposit of 1,108 USDT, bringing the final balance of **SUBJECT ADDRESS 2** to approximately 328,689.242732 USDT of which 60,901.6696 USDT is traceable to the transactions conducted by VICTIM 1. The remaining cryptocurrency is involved in money laundering, and thus subject to forfeiture.

*The Final Victim Transaction into **SUBJECT ADDRESS 1***

73. As previously described, VICTIM 1 made their final transaction on or about November 30, 2024, which was sent from their Coinbase account to DA 1. Those funds remained in DA 1 until the following day, December 1, 2024, when it was sent to CA 1.

Date	Amount	Hash	From	To
11/30/2024 20:05	20,895.49	0xe266aa7fa3b1c8b415a7673b1a49ac28193809661933f813865bacc52886a620	Coinbase	DA 1
12/1/2024 19:04	20,895.49	0x8f7a4ae6aef4df68f0bfed3c6a197b722b2adb6e9ee63a56f05b72f3bfe23cc9	DA 1	CA 1

74. Prior to this deposit, CA 1 held a balance of 5,619.064454 USDT, funds unrelated to VICTIM 1, but nonetheless likely from other scam victim(s). Upon receipt of the deposit, CA 1 held a balance of 26,514.557005. Minutes after receiving the deposit from DA 1, CA 1 sent approximately 26,000 USDT to **SUBJECT ADDRESS 1**.

Date	Amount	Hash	From	To
12/1/2024 19:09	26,000	0xe0dab2c493c49acc974dd7c1cc4bb9b339a93f654d5006160a408f55e0369369	CA 1	SA 1

75. Prior to this deposit, **SUBJECT ADDRESS 1** held a balance of approximately 0 USDT. Following this deposit, **SUBJECT ADDRESS 1**, held a balance of approximately 26,000 USDT. No additional transactions were conducted. Therefore, $20,895.49 of VICTIM 1 funds remain in **SUBJECT ADDRESS 1**. In addition, as all the funds currently held in **SUBJECT ADDRESS 1** are involved in money laundering, all of the funds are subject to forfeiture.

76. On December 4, 2024, the FBI requested Tether freeze the USDT remaining in **SUBJECT ADDRESS 1**. On December 6, 2024, Tether confirmed the address was blacklisted, the USDT was frozen, and the balance in **SUBJECT ADDRESS 1** was 26,000 USDT.

77. Between December 7-25, **SUBJECT ADDRESS 1** received 37,842.14415 USDT across 4 transactions. These funds were deposited into **SUBJECT ADDRESS 1** in a similar manner as the funds from VICTIM 1. Each transaction originated from an exchange, in this case all from Crypto.com, and were sent to a deposit address. Upon receipt, the deposit address then almost immediately transfers the funds, in the exact amounts, out of the address, and deposits them into **SUBJECT ADDRESS 1**. These funds are likely proceeds of fraudulent activities as described in this affidavit and are also involved in money laundering.

78. The foregoing establishes probable cause to believe that the funds held in the **SUBJECT ADDRESSES** are subject to civil and criminal forfeiture, as they contain proceeds of and property involved in cryptocurrency investment schemes, commonly referred to as pig butchering.

79. Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds associated with the Target Property. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would "burn" (i.e., destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with the Target Property and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

80. Based on information derived from the foregoing investigation, there is probable cause to conclude that the **SUBJECT ADDRESSES** received the proceeds of a wire fraud and money laundering scheme performed in violation of 18 U.S.C. §§ 1343, 1349 (wire fraud and conspiracy to commit wire fraud), and 18 U.S.C. § 1956(a)(1)(B)(i), 18 U.S.C. § 1957, and 18 U.S.C. § 1956(h) (money laundering, violation of the spending statute, and conspiracy to commit money laundering). Those proceeds are subject to forfeiture as proceeds of wire fraud, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), and as property involved in money laundering offenses, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1). Accordingly, I respectfully request that a warrant be issued authorizing the seizure of the **Subject Funds**.

81. A protective or restraining order issued pursuant to 21 U.S.C. § 853(e) may not be sufficient to ensure the availability of the funds in the **SUBJECT ADDRESSES.** Cryptocurrency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a "privacy" (i.e., untraceable) cryptocurrency. Thus, a seizure warrant is the only means to reasonably assure the availability of the funds in the **SUBJECT ADDRESSES** for forfeiture.

Respectfully submitted,

Michael Imbler
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) by telephone on 01/10/2025

Lindsey R Vaala Digitally signed by Lindsey R Vaala
Date: 2025.01.10 15:32:00 -05'00'

THE HONORABLE LINDSEY R. VAALA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency address(es). Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

a. All Tether ("USDT") held in a wallet address identified by 0x966913c26ab93a856f4b2372ecf6ba46a76e2b57

b. All Tether ("USDT") held in a wallet address identified by TPT4pz7g697maRahjUBvZHeSz2xvBaFCe6